**REMARKS**

In accordance with the foregoing, the claims 1, 3-4, 7, and 8-10 are amended and claims and new claims 11-19 are presented. Claims 1-19 are pending and under consideration.

**CLAIM AMENDMENTS**

Claims 1 and 8-10 are amended to recite a finite field corresponding to a mathematical finite aggregate having four defined arithmetical operations and a number of elements of the finite aggregate is expressed as $p^m$ where p is a prime number and m is a positive integer indicating an extension degree. (See, for example, page 1, lines 17-18 and page 2, lines 8-10).

Claims 3-4 are amended to correspond to parent claim 1.

Claim 7 is amended to correct informalities as suggested by the Examiner.

No new matter is presented in any of the foregoing and, accordingly, approval and entry of the amended claims are respectfully requested.

**NEW CLAIMS**

New claims 11-15 and 16-19 recite features of a data generating apparatus and method, respectively, reciting aspects of the present invention in an alternate fashion

No new matter is presented in any of the foregoing and, accordingly, approval and entry of the new claims are respectfully requested.

**ITEM 1: OBJECTION TO CLAIM 1**

Claims 7 is objected to since the term --stores-- was misspelled. Claim 7 is amended as suggested by the Examiner and withdrawal of the objection is requested.

**REQUEST FOR CLARIFICATION**

Applicants respectfully bring to the attention of the Examiner that Item 3, under the Page 2 heading of Claim Rejections -35 USC §102, states "Claims 2-7 are rejected as in claim 1." (Action at page 3). However, Item 3, pages 3-4 discusses only claims 2-3 and 6-7. Item 4 rejects claims 4-5 for obviousness under 35 U.S.C. 103(a) over Leppek in view of Wright, further conceding that "Leppek does not expressly disclose the generation of polynomial expressions." (Action at page 4).

Applicants request a clarification of Items 3 and Items 4.

To advance prosecution, Applicants response to the current Office Action assumes that the first line of Item 3 is in error and should not have included claims 4-5 in the rejection.

**ITEMS 2-3: REJECTION OF CLAIMS 1-3 AND 6-10 UNDER 35 U.S.C. §102(e) BY LEPPEK (U.S.P. 5,933,501)**

Independent claim 1 recites a data generating apparatus including an input device inputting a condition for designating a finite field and an expression data storage device storing the generated expression data.

Independent claim 8 recites a computer-readable storage medium on which is recorded a program enabling a computer to execute a process, the process including automatically generating expression data of a finite field.

Independent claim 9 recites a data generating method including designating a condition for designating a finite field, automatically generating expression data of the finite field based on the designated condition, and supplying the generated expression data to a finite field operation apparatus.

Independent claim 10 recites a data generating apparatus including inputting means for inputting a condition for designating a finite field, generating means for automatically generating expression data of the finite field based on the inputted condition, and expression data storing means for storing the generated expression data.

Further in claims 1, 8-10 (all as amended) the finite field corresponds to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as $p^m$ with p and m as a prime number and a positive integer indicating an extension degree, respectively.

The Examiner contends that Leppek describes "designating a finite field (column 4 lines 33-51)." (Action at pages 2 and 3). The Examiner also contends that Leppke describes an "expression storage device storing generated expression data (column 4 lines 7-23)" and "expression data storing means for storing the generating expression data (column 4 lines 52-56)." (Action at pages 2 and 3).

**Traverse**

As provided in MPEP §706.02 entitled Rejection on Prior Art, anticipation requires that the reference must teach every aspect of a claimed invention. Leppek does not support an anticipatory-type rejection by not describing features recited in the present application's independent claims.

**Designating A Finite Field Not Described**

Applicants submit that Leppek does not describe a <u>finite</u> field as the Examiner contends,

but only an encryption of data for transmission and a plurality of different encryption operations combined into a compound sequence of encryption operations. Leppek, in fact, describes (col. 4 lines 34-50), in the lines cited by the Examiner:

> an encryption driver or key 170 comprised of a sequence of M access code entries made up of K (at least two and up to all N) . . . M may be any number equal to or greater than two. . . . Even if N is only two, M is still unbounded, since it may comprise an alternating sequence of arbitrary length. . . M could be generated as the alternating sequence . . . , 120-1, 120-2, 120-1, 120-2, 120-1, 120-2, 120-1, 120-2, . . . , up to M entries, where M>2.

That is, if a field is *arguendo* described, such a field is not a finite field, but rather an infinite field, let alone a finite field that corresponds to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as $p^m$ with p and m as a prime number and a positive integer indicating an extension degree, respectively.

**Storage Device Storing Generated Expression Data And Expression Data Storing Means Storing Generated Expression Data Not Described**

Applicants submit that Leppek does not describe either a storage device storing a generated expression or an expression data storing means storing generated expression data as the Examiner contends. Leppek only describes (cols. 4-5, starting at line 19):

> a memory access controller of a supervisory encryption assembly manager 130 to call up or retrieve a respective encryption operator 120-i in the course of generating an encryption operator sequence 140 that operates on a data stream 150 to be transmitted . . . the first operator entry 110 associated with the first code of the sequence 140 and applies the data 150 . . . This successive process of accessing sequentially differing encryption operators and wrapping the previously encrypted data continues until the last access code in the encryption control sequence 140 is processed. The compound-encrypted data is then transmitted over communication path . . .

(Emphasis added).

That is assuming *arguendo* that an expression or expression data are generated, Applicants submit that such generated expression or generated expression data are communicated and not stored.

**Features of Dependent Claims Not Described**

For example, dependent claim 3 recites when a bit length of a prime number that describes the finite field is inputted as the condition, the generation device automatically generates prime number data corresponding to the bit length and stores the generated prime number data in said expression data storage device. Applicant submits these features are not described, nor does the Examiner contend such features are explicitly described in the cited art.

The Examiner contends only that Leppek uses different encryption routines. (Action at page 2). According to the Office Action, without providing any basis from a reference, the Examiner further contends that:

> one well known example is the RSA encryption routine, which uses random keys. The size of the keys is a design choice. The keys are inherently developed using a random number generator, which would generate them automatically.

(Action at page 3).

However, as set forth in MPEP §2144.03 entitled Reliance on Common Knowledge or "Well Known" Prior Art while:

> "official notice" may be relied on, these circumstances should be rare when an application is under final rejection or action under 37 CFR 1.113. Official notice unsupported by documentary evidence should only be taken by the examiner where the facts asserted to be well-known, or be common knowledge in the art are capable instant and unquestionable demonstration as being well-known.

The Office Action has provided no explicit support of how the determination of features as being well-known has been determined.

Dependent claim 6 recites a generation device storing expression data of a finite field corresponding to a condition in a expression data storage device, and the generation device automatically generating expression data of the finite field corresponding to the condition if there is no expression data of the finite field corresponding to the condition in the fixed data storage device. The Examiner contends that:

> (the) generator, of the Leppek system, always constructs the expression from the access code data using the stored information in the fixed storage such as 100.

However, Leppek only describes:

> database 100 containing a plurality of respectively different data encryption routine or operator entries.

Applicants submit there is no description in Leppke of a generator device storing expression data corresponding to a condition in an expression storage device, nor has the Examiner cited such a description.

Dependent claim 7 recites a verifier device verifying whether the designated expression data are suitable, the verifier device storing the designated expression data in said expression data storage device if the designated expression data are suitable, and the verifier device asking the designation device for other expression data if the designated expression data are not suitable. The Examiner contends this is described in Leppke (claim 5 lines 19-33), and that the:

> supervisory encryption assembly manager processes the sequence and therefore is responsible for verifying that the encryption process is carried out as designed.

However, nowhere in the lines cited by the Examiner, or anywhere else in Leppke, is a

verifying device as recited in claim 7 described. In fact, Leppke does not use the term--verify-- at all.

**Conclusion**

Since Leppek does not describe features recited in independent claims 1 and 8-10, and in the dependent claims, the rejections should be withdrawn, and claims 1-10 allowed.

**ITEMS 4-5: REJECTION OF CLAIMS 4-5 FOR OBVIOUSNESS UNDER 35 U.S.C. §103(a) OVER LEPPEK IN VIEW OF WRIGHT (PAPER A RANDOM POLYNOMIAL GENERATOR, July 14, 1994, PAGES 1-9)**

Claims 4 and 5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Leppek as applied to claim 1 above, and further in view of Wright. (Action at page 4).

Dependent claim 4 recites a data generating apparatus wherein when an extension degree which describes a finite field is inputted as the condition a generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device.

Dependent claim 5 recites that when an instruction using an optimal normal basis is inputted, the generation device automatically generates irreducible polynomial data for an optimal normal basis corresponding to the extension degree and the irreducible polynomial data for an optimal normal basis in said expression data storage device.

The Action concedes that Leppek does not expressly disclose the generation of polynomial expressions. (Action at page 4). However, the Examiner contends this feature is described by Wright and there is motivation to modify Leppek. (Action at page 5).

***Prima Facie* Obviousness Not Established**

**Generation Device Automatically Generating Irreducible Polynomial Data Corresponding To An Extension Degree Not Described Or Taught By The Cited Art Alone Or In Combination**

As provided in MPEP §2143.03 "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F. 2d 1981, (CCPA 1974)."

Neither Leppke or Wright describe a generation device automatically generating data corresponding to an extension degree.

Leppek only describes a:

> successive process of accessing sequentially differing encryption operators and wrapping the previously encrypted data continues until the last access code in the encryption control sequence 140 is processed.

Since feature of the claims are not described by the cited art alone, or in combination, the rejection to claims 4-5 should be withdrawn.

**NEW CLAIMS**

New claims 11-15 recite a data generating apparatus including an input device inputting a condition for designating a finite field, and an expression data storage device storing expression data of the finite field, wherein the expression data is based on based on the inputted condition.

New claims 16-19 recite a data generating method designating a condition for a finite field, generating designated expression data of the finite field based on the designated condition, and storing the generated designated expression data.

These, and other, features of claims 11-19 are patentably distinguishable from the cited art, and they are submitted to be allowable for the recitations therein.

**CONCLUSION**

No new matter is presented in any of the foregoing and, accordingly, approval and amended claims, and new claims are respectfully requested.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 5, 2004

By: Paul W. Bobowiec

Paul W. Bobowiec
Registration No. 47,431

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501